Virus Def'n 20

Suspect Files 22

4

Remote Site Server

Virus Source

6

Internet Link 8

10

Firewall Server 16

File Server 12

Mail Server 18

2

Client

Client

Client 14

Client

Client

Client

Client

Fig. 1

CPU 24

RAM 26

Non-volatile Storage 22

External Network Link 30

38

Internal Network Link 36

Display Driver 32

User Input 34

OD 44

40

42

Fig 2

Fig. 3

Start

Get current
thresholds &
tests — 46

Select First
threshold & test — 48

Detect measurement
parameter MPn — 50

MPn crossed
Thn? — 52

Y → Signal
Virus
Outbreak — 54

N

Last
test? — 56

N → Select next
threshold & test — 58

Y

End

Fig. 4

Virus Outbreak Detected

↓

Execute Step 1

Confirm Step 2 — Escalation time 1

Execute Step 2

Execute Step 3 — Escalation time 2
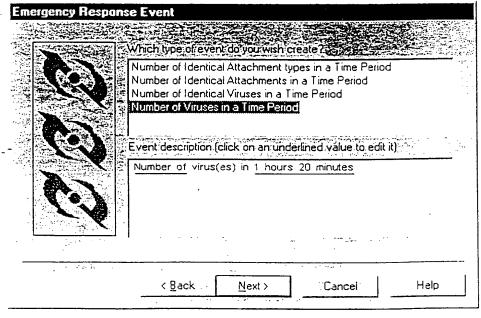
Execute Step 4 — Escalation time 3

Confirm Step 5 — Escalation time 4

Execute Step 6

Fig. 5

Start

Get current
sequence — 60

Select First
step — 62

User
confirmation
received?
55

N

Y

Confirmation
required? — 64

Y

N

Execute
step — 68

Wait
escalation
time — 70

Output
continues? — 72

N

Y

Last
step? — 74

N

Select
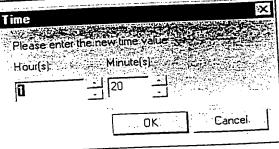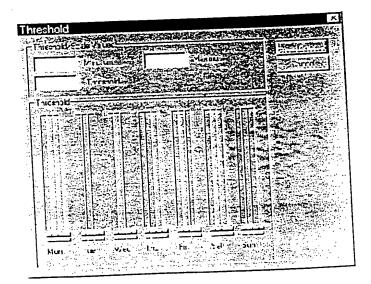next
step — 76

Y

End

Fig. 6

Network Associates Emergency Response [X]

Apply rules in the following order

Outbreak response stage 1
Outbreak response stage 2

New

Copy

Modify

Rename...

Delete

Move Up   Move Down

Event description (click on an underlined value to edit it)

OK   Cancel

Fig 7

Emergency Response Event

Which type of event do you wish create?

Number of Identical Attachment types in a Time Period
Number of Identical Attachments in a Time Period
Number of Identical Viruses in a Time Period
Number of Viruses in a Time Period

Event description (click on an underlined value to edit it)

Number of virus(es) in 1 hours 20 minutes

< Back   Next >   Cancel   Help

Fig 8

Number

Please enter the new numeric value

5

OK   Cancel

Time

Please enter the new time value

Hour(s):   Minute(s):

1   20

OK   Cancel

Fig. 9

Threshold

Threshold Code Value

Threshold

Mon   Tue   Wed   Thu   Fri   Sat   Sun

Fig. 10

Emergency Response Event

Which type of reaction do you wish for this event?

○ Manual
○ Automatic

☑ Notify by email
☐ Notify by network broadcast
☐ Notify by pager

Reaction description (click on an underlined value to edit it)

React manually to an emergency response but notify me via email address <u>email address</u>

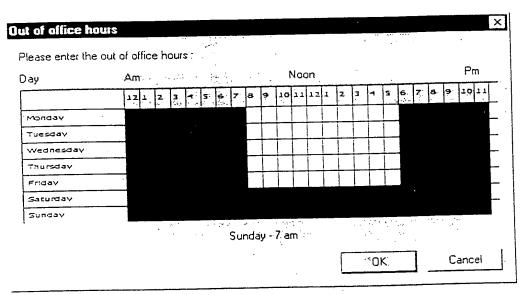| < Back | Next > | Cancel | Help |

Fig. 11

Number ✕

Please enter the new numeric value :

3028423555111

| OK | Cancel |

Fig. 12

Email Address ✕

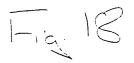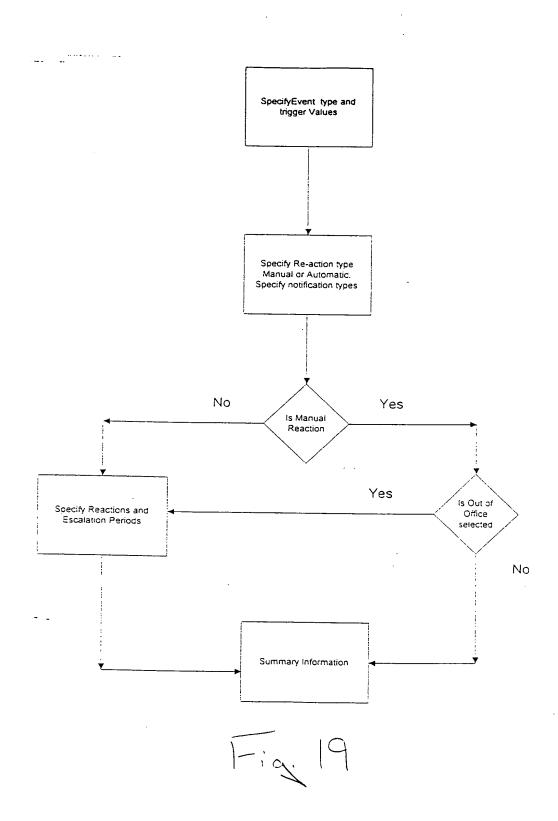Please enter the new email address :

a@a.com

| OK | Cancel |

Fig. 13

Machine name ✕

Please enter the new machine name:

AYL-NOBODY

[OK] [Cancel]

Fig. 14

Out of office hours ✕

Please enter the out of office hours :

Day	Am										Noon										Pm	
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								
Sunday																								

Sunday - 7 am

[OK]   Cancel

Fig. 15

Emergency Response Event

Specify the actions and step to carry out:

Step	Action	Escalation Time
0	Update DAT files (GroupShield Exc...	0 hr(s) 1 min(s)
1	Reduce notifications (GroupShield ...	0 hr(s) 10 min(s)

Move Up | Move Down | Add | Remove

☐ Create an emergency response report

< Back | Next > | Cancel | Help

Fig. 16

Available [Acti]ons

Component	Action
GroupShield Exchange	Delete on Infection
GroupShield Exchange	Reduce notifications
GroupShield Exchange	Hide Mailboxes
GroupShield Exchange	Hide distribution lists
GroupShield Exchange	Perform On-Demand Scan
GroupShield Exchange	Update DAT files
GroupShield Exchange	Down the Exchange Server
GroupShield Exchange	Increase Scanning Options

Escalation Time

Escalate after:: [0] hr(s) [0] min(s)

[OK]   [Cancel]

Fig. 17

Emergency Response Event

Specify the name for this event:

[Event1]

Event Summary

Event Name : Number of Identical Attachment types in a Time f
Event Desc : 500 identical attachment types in 1 hours 20 min
Reaction to an Emergency is Automatic
Email Notification is Enabled. Email will be sent to 'a@a.com'.

Automatic Actions:

Step, Action and escalation times.

0   Update DAT files (0 hr(s) 1 min(s))

[< Back]   [Finish]   [Cancel]   [Help]

Fig. 18

```
                    ●                           ●


                              ┌─────────────────────┐
                              │  SpecifyEvent  type and │
                              │    trigger Values       │
                              │                         │
                              └───────────┬─────────────┘
                                          │
                                          │
                                          │
                              ┌───────────▼─────────────┐
                              │  Specify Re-action type  │
                              │  Manual or Automatic.    │
                              │  Specify notification types│
                              └───────────┬─────────────┘
                                          │
                                          │
             No                          ◇                      Yes
      ◄──────────────────────    Is Manual    ──────────────────────►
                              Reaction
                                          ◇


  ┌──────────────────────┐                           ◇
  │ Specify Reactions and│       Yes           Is Out of
  │ Escalation Periods   │◄────────────────     Office         No
  │                      │                      selected   ────────►
  └──────────┬───────────┘                          ◇
             │
             │
             │                ┌─────────────────────┐
             │                │                      │
             └───────────────►│  Summary Information  │◄──────────
                              │                      │
                              └─────────────────────┘
```

Fig. 19

Fig. 20

Fig. 21

Attachment Name	Attachment Size	Occurences	Virus Type	Virus Name	Time	
ABC.doc	1034	2	MACRO	WMCAP	10:45:45	OK
XYZ.exe	4096	10	FILE	Bomber	21:19:32	Cancel

Outbreak Statistics

Fig. 22

Lockdown ☒

Network Associates has determined a virus Outbreak based on the currently defined triggers. What action would you like to take?

[OK]
[Cancel]

○ None

○ Turn down notification options to reduce load on the server

○ Increase security on scanning options

○ Perform a DAT update to retrive latest detection and cleans in

○ Perform an on-demand scan

○ Block all attachments by trigger

○ Perform an on-demand scan

○ Allow only one Admin to logon to Exchange

○ Down Exchange.

Recommendation by GroupShield :

Perform an dat update from Network Associates FTP stie.

Fig 23